

# 周报 2019.4.15~4.21

Done

## 1.调研联邦学习

- OneNote共享笔记: <https://1drv.ms/o/s!AssDZciLN1gxjGpGOM0Q2jQQYkCd>
- 一些基本概念:

## 联邦迁移学习的基本概念

[机器之心专访杨强教授：联邦迁移学习与金融领域的AI落地](#)

### 研究原因

- 欧盟通过了「数据隐私保护条例」(General Data Protection Regulation, 简称GDPR), 大数据公司不能直接互相交流用户数据, 对依赖数据的机器学习是一个巨大挑战。
- 因此, 需要在保护用户数据隐私、合法合规的前提下, 继续进行机器学习。
- **联邦学习 (Federated Learning)**: 在不共享数据的前提下, 利用双方的数据实现模型增长

### 方法

1. 假设两家公司想要建立一个用户画像模型, 其中部分用户是重合的。
2. 首先通过加密交换的手段, 建立用户的识别符 (identifier) 并进行沟通, 在加密状态下用减法找出共有的部分用户。因为关键用户信息并没有得到交换, 交换的只是共有的识别符, 因此这并不违反GDPR。
3. 然后, 双方将这部分数据提取出来, 将各自拥有的同样用户的不同特征作为输入, 迭代地进行训练模型、交换参数的过程。
4. 我们证明了给定模型参数, 双方不能互相反推出对方拥有的、自己没有的特征, 因此用户隐私仍然得到了保护。在不违反 GDPR 的情况下, 双方的模型性能都得到了提高。

### 和迁移学习的比较

- 迁移学习存在**性能损失**, 从领域A迁移到领域B时会丢失领域A的一大部分知识, 甚至负迁移。
- 但是, 联邦学习保证**无损失**, 交流的公司A和公司B能在加密信息交换系统的管理下, 同时成长。就像美国的不同州在联邦政府的管理下。这称作**联邦迁移学习 (Federated Transfer Learning)**。

## 2.ChinaVis 2019 挑战赛 项目

- 官网: <http://www.chinavis.org/2019/index.html>
- 小组四人, 参加挑战赛1, 6月10日前完成提交
- 需要学习React, Redux, KOA的使用

## 小结

这周开始参加微众银行项目，先调研联邦学习；参加ChinaVis挑战赛；此外5月24日的组会报告、毕业设计也要同时进行。

## Plan

### 短期计划

1. 先看联邦学习、迁移学习的概念，再看实现方法和样例
2. 先学习react相关知识，再修改ChinaVis2019的前端

### 中期计划

1. 写本科毕业设计
2. 写组会报告

### 长期计划

1. 6月份时，完成上述几个事项